

**BY ORDER OF THE COMMANDER  
482D FIGHTER WING**

**482D FIGHTER WING INSTRUCTION  
10-701**



**24 OCTOBER 2011**

***Operations***

**OPERATIONS SECURITY (OPSEC)**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**ACCESSIBILITY:** Publications and Forms are available for downloading or ordering on the e-publishing website at <http://www.e.publishing.af.mil/>.

**RELEASABILITY:** There are no releasability restrictions on this publication.

---

OPR: 482 FW/IP

Certified by: 482 FW/CV  
(Col David R. Davis)

Pages: 6

---

This instruction establishes procedures and responsibilities to implement Operations Security (OPSEC) for the 482d Fighter Wing (482 FW) and to accomplish the intent of Air Force Instruction (AFI) 10-701, *Operations Security (OPSEC) Instructions*, and AFI 10-701\_Air Combat Command Supplement 1(ACC), *Operations Security (OPSEC)*. It applies to all 482 FW personnel. Tenant units will comply in accordance with agreements between the tenant unit commander and 482 FW. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the Air Force Form 847 (AF Form 847), *Recommendation for Change of Publication*; route AF Form 847 from the field through the appropriate functional's chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at <https://www.my.mil.gcscs-af61a/afrims/afrims/rims.cfm>.

**1. The Goal of OPSEC.** Identify critical unclassified information from the wing's daily and wartime operation which could give an adversary an advantage if exploited. Determine the threat and the ways in which this information could be collected or exploited. Assess the level of damage that would occur to wing operations if this information is successfully exploited and assess the risk. If the risk level is not acceptable, find ways to prevent the adversary from exploiting the information or deny them an advantage. OPSEC is an analytical tool which should be used in planning and operation of all wing activities.

**2. Responsibilities:**

2.1. The 482d Wing Commander will:

2.1.1. Appoint a 482 FW Signature Management Officer (SMO) who will function as the OPR for all Signature Managers (SM) activities. The primary SMO will be an O-3 or above, or civilian equivalent.

2.1.2. Appoint a Wing Signature Management Alternate, either Officer or Non-Commissioned Officer (SMNCO). The alternate SMO will be an E-6 or above, or civilian equivalent.

2.1.3. Sign a memorandum for record describing the wing's OPSEC policy.

2.1.4. Determine the wing's Critical Information List (CIL).

2.2. The 482 FW/SMO will:

2.2.1. Ensure wing level OPSEC procedures and requirements are in compliance as directed by AFI 10-701 and ACC supplements.

2.2.1.1. Advise the installation commander on OPSEC issues as required.

2.2.2. Act as the focal point for OPSEC and provide guidance and assistance to wing units in ensuring compliance with the wing program.

2.2.3. Assist the installation commander in developing the wing's CIL. The SMO will review and update the CIL and indicators as necessary.

2.2.4. Ensure OPSEC is closely coordinated with security disciplines in the wing.

2.2.5. Review 482 FW operations plans to ensure a statement of OPSEC considerations and appropriate essential elements of friendly information (EEFIs) are included.

2.2.6. Submit OPSEC reports to higher headquarters as directed.

2.2.7. Chair the OPSEC Working Group (OWG) meetings.

2.2.8. Oversee the Wing OPSEC training program.

2.2.8.1. Ensure the unit level OPSEC Coordinators are appropriately trained within 90 days of appointment.

2.2.8.2. Ensure that all military, civil service and base operating support (BOS) contractors newcomer's receive initial and annual training.

2.2.9. Complete the wing OPSEC self-inspection annually.

2.2.10. Maintain the wing OPSEC continuity book.

2.3. Unit commanders will:

2.3.1. Take an active role to ensure the success of the wing OPSEC program.

2.3.2. Appoint an OPSEC Coordinator and alternate to administer the unit's OPSEC program.

2.3.3. Forward a copy of the unit's letter of appointment to the wing OPSEC program manager.

2.3.4. Develop a Critical Information List (CIL) specifically tailored to the unit mission, using guidance provided by the wing SMO. For some organizations, it may be necessary

to develop a CIL for each work center. Other organizations may be able to develop one CIL that is applicable to all unit work centers.

2.3.5. Ensure newly assigned unit OPSEC Monitors are briefed by the wing SMO.

2.4. Unit OPSEC Coordinators will:

2.4.1. Contact the Wing SMO upon being appointed to schedule an initial briefing.

2.4.2. Maintain current copies of this instruction and AFI 10-701 and applicable supplements, and become knowledgeable on the content of the publications.

2.4.3. Assist the Commander in building a unit CIL.

2.4.4. Ensure the unit's CIL and 482 FW CIL is readily available to all unit personnel.

2.4.5. Train the alternate OPSEC Coordinator on all aspects of the unit OPSEC program. The alternate must be able to effectively manage the entire program when the primary monitor is absent.

2.4.6. Ensure all personnel assigned to the unit receive OPSEC training within 90 days after reporting.

2.4.7. Ensure all OPSEC training is accomplished and documented in the AF Advanced Distributed Learning Service (ADLS) website (<https://golearn.csd.disa.mil>).

2.4.7.1. Organizational specific training will be provided in addition to this training to ensure all personnel in the Air Force are aware of local threats, vulnerabilities and critical information unique to their duty assignment.

2.4.8. Disseminate information and guidance from the 482 FW/SMO/SMNCO and implement/execute the 482 FW OPSEC program.

2.4.9. Attend and participate in wing OWG meetings as directed by the 482 FW/SMO/SMNCO. The unit coordinator will forward any OPSEC issues to the wing OPSEC manager and the OPSEC working group.

2.4.10. Assist the wing OPSEC manager in the review of the critical information list and any surveys which affect the unit.

2.4.11. Conduct an annual review of the unit's OPSEC procedures and report it to the SMO.

2.4.11.1. Complete the unit/wing OPSEC self-inspection checklist annually.

2.4.12. Maintain a continuity book as required.

2.5. Base Operation Support ( OPSEC) Manager.

2.5.1. The BOS OPSEC Coordinator and their alternate will be appointed by memorandum. The primary must be in a position which allows them to oversee the sections of the contractor which play a role in the daily and wartime operations of the wing (i.e., Base Operations, Weather, etc.).

2.5.2. Ensure the BOS contractor and its full-time employees are complying with all OPSEC directives.

2.5.3. Provide and document all BOS OPSEC training when directed or needed as outlined in [2.4.7](#)

2.5.4. Provide reminders throughout the year for BOS members to practice good OPSEC and promote OPSEC awareness within the BOS contractor.

2.5.5. Train all new fulltime BOS personnel on OPSEC practices and thoroughly brief them on the Critical Information List and counter measures.

2.5.6. Forward any OPSEC issues to the wing OPSEC manager and the OPSEC working group.

2.5.7. Assist in any OPSEC surveys or assessments which affect the BOS contractor.

2.5.8. Complete an OPSEC self-inspection checklist annually.

## 2.6. 482 FW Public Affairs (PA).

2.6.1. The 482 FW Public Affairs office has a unique position in protecting Critical Information while at the same time complying with the Department of Defense (DoD) Principles of Information, PA core competencies, and PA's role in Information Operations. Open communication between the SMO and the Chief of Public Affairs must be maintained to have an effective OPSEC program.

2.6.2. Public Affairs will appoint a primary and alternate OPSEC representative in writing to help protect Critical Information during day-to-day operations and to conduct regular section training.

2.6.3. Public Affairs will inform the SMO of higher headquarters policy and guidance (PAG) on critical information approved for release to the public and media.

2.6.4. The 482 FW/PA OPSEC representative will ensure media releases do not contain Critical Information outside the scope of information approved for release by higher headquarters. The Chief of Public Affairs will consult with the wing SMO or alternate prior to the release of critical information.

2.6.5. Will utilize the OPSEC "5 Step Process" to mitigate risk. 1) Identify critical information; 2) Analyze threats; 3) Analyze vulnerabilities; 4) Assess risk; and 5) Apply countermeasures. Although normally applied in a sequential manner the process during deliberate or crisis action planning, dynamic situations may require any step to be revisited at any time.

2.6.6. Attend and participate in wing OWG meetings as directed by the 482 FW/SMO/SMNCO.

## 2.7. OPSEC Working Group.

2.7.1. The OPSEC working group will be appointed by memorandum from the installation commander. It will include, as a minimum: intelligence, antiterrorism, force protection, information protection, and PA. The working group will meet annually, during initial planning phase of any 482 FW exercises, deployments, and major events, or as directed by the installation commander.

2.7.2. Periodically review the wing's CIL.

2.7.3. Assist in any OPSEC surveys or assessments.

2.7.4. Pass any recommendations to the appropriate wing, group or unit agency.

2.8. Functional Areas.

2.8.1. Functional areas not covered in specific sections, such as Financial Management (FM), Legal Affairs (JA), or Family Support, will fall under the FW/SMO. They will designate an OPSEC Coordinator if manning permits and will develop a CIL when directed by the FW/SMO.

**3. Procedures:**

3.1. All “newcomers” will receive initial OPSEC training. Organization-specific initial OPSEC awareness training will be provided at each new duty location as part of in-processing and annually thereafter, at a minimum.

3.1.1. Air Force personnel military, civilian, and contractors who have access to mission critical information require OPSEC training. This is accomplished through initial and annual OPSEC training. Standardized AF OPSEC awareness training is located on the AF Advanced Distributed Learning Service (ADLS) under the Annual Total Force Awareness Training (TFAT) Information Protection block.

3.1.2. Personnel must understand the scope of the threats, the nature of the vulnerabilities and their responsibility to execute countermeasures to protect critical information and organization specific OPSEC indicators. Annual training must include, at a minimum, updated threat and vulnerability information, changes to critical information and new procedures and/or countermeasures implemented by the organization.

DONALD R. LINDBERG, Colonel, USAFR  
Commander

**Attachment 1****GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

AFI 10-701, *Operations Security (OPSEC) Instructions*, 8 June 2011

AFI 10-701, ACC Sup 1, *Operations Security (OPSEC)*, 22 January 2009

AFMAN 33-363, *Management of Records*, 1 March 2008

***Adopted Forms***

AF Form 847, *Recommendation for Change of Publication*

***Acronyms***

**ACC**—Air Combat Command

**ADLS**—Advanced Distributed Learning Services

**AF**—Air Force

**AFI**—Air Force Instruction

**AFMAN**—Air Force Manual

**AFRC**—Air Force Reserve Command

**BOS**—Base Operation Support

**CC**—Commander

**CIL**—Critical Information List

**CV**—Vice Commander

**DoD**—Department of Defense

**FW**—Fighter Wing

**IAW**—In Accordance With

**OPR**—Office of Primary Responsibility

**OPSEC**—Operations Security

**OWG**—Operations Security Working Group

**PA**—Public Affairs

**RDS**—Records Disposition Schedule

**SM**—Signature Management

**SMO**—Signature Management Officer

**SMNCO**—Signature Management Noncommissioned Officer

**TFAT**—Total Force Awareness Training